全球数据安全观察

总第 84 期 2022 年第 12 期

(2022.04.04-2022.04.10)

目录

政策形势	1
1、全国首项《网络数据安全监督检查规范》地方标准公开征求意见.....	1
2、《重庆市数据条例》建立数据安全责任制.....	1
3、银保监会：外部涉企数据要关注数据源合规.....	2
4、《广州市数字经济促进条例》公布，为首席数据官、数据经纪人等创新试点提供法律保障.....	3
5、证监会：加强保密和档案管理，明确上市公司信息安全责任.....	4
6、美国《犹他州消费者隐私法》(UCPA)通过，成为第四部州级全面隐私立法.....	5
7、欧盟和美国就新的《跨大西洋数据隐私框架》达成原则性协议.....	5
8、欧洲议会通过《数据治理法案》，促进欧盟数据共享新规则.....	6
技术、产品与市场	8
1、360 核心安全大脑 3.0 正式发布，构建政企用户的“能力中枢平台”.....	8
2、IBM 发布业界首款量子安全平台 IBM z16.....	9
3、《2021 年度数据泄漏态势分析报告》发布.....	10
4、零信任的行业应用场景分析研究.....	10

大数据协同安全技术国家工程研究中心

5、非可信环境下的云端数据加密与授权方案	11
业界观点.....	12
1、王云鹏院士：探索构建包容审慎的汽车安全监管沙盒.	12
2、陈兵：车企须在让渡隐私与获得便利性间找平衡点	13
3、专家解读：与时俱进 筑牢国家安全的审查防线	14
4、保护个人信息，给“算法应用”立规矩.....	15
5、依法应对元宇宙发展中的风险挑战	17
数据安全事件	19
1、爱尔兰银行因数据泄露被罚款 463,000 欧元.....	19
2、Lapsus\$再出手：泄露 Globant 软件公司 70GB 数据	19
3、Conti 团伙泄露从 Parker Hannifin 窃取数 GB 文件	20
4、美国国防承包商关联公司借激励计划名头，通过 SDK 收集用户敏感数据.....	20
5、俄罗斯外卖应用的泄露数据中包含 GRU 特勤人员的用餐习惯.....	21
6、黑客通过虚假购物应用程序以窃取马来西亚用户的银行数据.....	22
7、福克斯新闻泄露 1300 万条数据，包含员工信息	22
8、Cash App 数据泄露恐将影响 820 万美国用户	23
9、得克萨斯州保险部泄露了 180 万人的数据	24
10、西班牙 Iberdrola 遭到攻击泄露 130 万客户的数据	24

政策形势

1、全国首项《网络数据安全监督检查规范》地方标准公开征求意见

日前，全国首项《网络数据安全监督检查规范（征求意见稿）》由天津市市场监督管理委员会发布，正式向社会各界公开征求意见。《网络数据安全监督检查规范（征求意见稿）》共七章分别为：范围、规范性引用文件、术语和定义、监督检查流程、监督检查方式、监督检查要求、监督检查结果。

《网络数据安全监督检查规范（征求意见稿）》主要规定了网络数据安全监督检查的流程、内容和要求，主要适用场景为对网络数据处理者网络数据的收集、存储、使用、加工、传输、提供、公开等活动进行监督、检查、管理和评估。该项标准不仅适用于主管部门、监管部门、第三方评估机构，从作为数据处理者的企业角度来看，同样也适用于企业开展建设、自查以及整改工作。

<https://mp.weixin.qq.com/s/Fwq9oYsXmglSZEhdMOGIIfQ>

2、《重庆市数据条例》建立数据安全责任制

3月30日，《重庆市数据条例》（以下简称条例）经市

五届人大常委会第三十三次会议表决通过,将于 2022 年 7 月 1 日起施行。条例分为总则、**数据处理和安全**、数据资源、数据要素市场、发展应用、区域协同、法律责任、附则,共 8 章,60 条。条例以促进数字经济发展、有效破除数据壁垒为抓手,在数据资源开发应用、推动数据技术创新、数据区域协作等方面进行探索创新。条例在落实国家数据要素市场化配置改革基础上,聚焦数据要素市场培育,促进数据要素流通、交易等。条例还明确了公共数据的范围,条例第三条规定,公共数据是政务数据和公共服务数据的统称。条例提出:政务数据是国家机关和法律、法规授权的具有管理公共事务职能的组织为履行法定职责收集、制作的数据;公共服务数据是医疗、教育、供水、供电、供气、通信、文旅、体育、环境保护、交通运输等公共企业事业单位在提供公共服务过程中收集、制作的涉及公共利益的数据。

<https://mp.weixin.qq.com/s/u3bh8NbwuCTZ-X1cNWkoKw>

3、银保监：外部涉企数据要关注数据源合规

4 月 6 日,银保监会发布《中国银保监会办公厅关于 2022 年进一步强化金融支持小微企业发展工作的通知》。通知指出外部涉企数据要关注**数据源合规**:一是依据小微企业生产经营和融资渠道高度本地化的特点,明确重点提高区域性信

息集成共享和应用效率。二是银行保险机构要提升数据管理能力，确保业务经营、产品研发、风险管理、内部控制的关键环节自主把控。三是通过各级融资信用服务平台获取的涉企信用信息不得用于为企业提供融资支持以外的活动。四是通过第三方机构获取外部涉企数据的，要关注数据源合规风险，明确数据权属关系，加强数据安全技术保护。

https://mp.weixin.qq.com/s/NaQHKgpAvd6uD_Sfs9O2eg

4、《广州市数字经济促进条例》公布，为首席数据官、数据经纪人等创新试点提供法律保障

4月6日，广州市人大常委会发布公告，《广州市数字经济促进条例》（简称《条例》）经广东省人大常委会批准，自2022年6月1日起施行。

《条例》共八十九条，以推动数字产业化和产业数字化发展为核心，加强数字基础设施建设、数据资源价值化、提升城市治理数字化水平，为广州建设成为具有全球影响力的数字经济引领型城市提供了法治保障。

值得关注的是，《条例》针对首席数据官、数据经纪人等创新试点提供了法律保障，明确提出“建立健全部门协同、市区联动、政企合作的数据治理体制机制，探索推行首席数据官等数据管理创新制度”，“探索建立数据交易平台、场

所以及数据入场规范、数据经纪人管理等配套制度”。

<https://mp.weixin.qq.com/s/hZCvXLvBG3XiC0bQFY5jzA>

5、证监会：加强保密和档案管理，明确上市公司信息安全责任

4月2日，证监会公布《关于加强境内企业境外发行证券和上市相关保密和档案管理工作的规定(征求意见稿)》(以下简称《规定》)，向社会公开征求意见。

本次修订，将为境外上市涉及的相关保密和档案管理工作提供更加清晰的指引，便利有关市场主体依法依规高效开展境外发行上市活动；将指导企业**妥善管理涉密和敏感信息**，履行好维护国家信息安全的主体责任；也将有助于相关监管部门与境外监管机构安全高效开展包括联合检查在内的跨境监管合作活动，共同维护全球投资者权益。证监会负责人表示依法依规做好涉密敏感信息的管理，落实信息安全主体责任，是企业合规经营的重要内容。从实践情况看，企业向有关证券公司、证券服务机构提供包含涉密或敏感信息的文件、资料应属极少数情况。如因审计工作需要确有必要提供的，《规定》重申企业须按照相关法律法规履行必要的审批或备案程序，并要求企业保留履程序程和提供信息的相关记录并向中介机构提供书面说明，不会给企业带来过高的合规

成本。《规定》的落实，将提升企业维护信息安全和防范法律风险的能力，促进企业依法合规开展境外发行上市活动。

<https://mp.weixin.qq.com/s/a1tyI28dVIpEQdvqhLhqQw>

6、美国《犹他州消费者隐私法》(UCPA)通过，成为第四部州级全面隐私立法

3月24日，美国犹他州州长 Spencer Cox 签署了《犹他州消费者隐私法》(UCPA)，使犹他州成为第四个颁布全面消费者隐私立法的州。该法于2023年12月31日生效。

UCPA 与加利福尼亚州、弗吉尼亚州和科罗拉多州的消费者隐私法既相似又不同。它在很大程度上借鉴了《弗吉尼亚州消费者数据保护法》(VCDPA)，与《科罗拉多隐私法》(CPA)也有类似部分。UCPA 适用于任何控制者或处理者，通过包括多个门槛要求，UCPA 的范围与其他州的现行隐私法相比更窄。

<https://mp.weixin.qq.com/s/huk8KNQf7Z5ZdFgxEjnj3A>

7、欧盟和美国就新的《跨大西洋数据隐私框架》达成原则性协议

欧盟委员会和美国宣布：欧美已就新的《跨大西洋数据隐私框架》达成原则性协议，该框架将促进跨大西洋数据流

动，并解决欧盟法院在 2020 年 7 月的 Schrems II 裁决中提出的关切。

新《跨大西洋数据隐私框架》标志着美国方面作出了前所未有的承诺：将实施改革，加强适用于美国通讯情报活动的隐私和公民自由保护。根据《跨大西洋数据隐私框架》，美国将制定新的保障措施，以确保通讯监视活动在追求确定的国家安全目标是必要的和相称的，建立一个具有指导补救措施的有约束力的两级独立机制，并加强对通讯情报活动的严格分层监督，以确保遵守对监视活动的限制。

https://mp.weixin.qq.com/s/HUqyKvp65hFxujetBG3L_g

8、欧洲议会通过《数据治理法案》，促进欧盟数据共享新规则

4 月 6 日，欧洲议会就欧盟《数据治理法案》（Data Governance Act; 简称“DGA”）进行最终投票表决。最终，《数据治理法案》以 501 票赞成 VS12 票反对、40 票弃权，获得议会批准。

根据欧盟委员会的数据，公共机构、企业和公民产生的数据量预计将在 2018 年至 2025 年间增加五倍。基于《数据治理法案》形成的新规则将允许欧盟更好地使用这些数据，预计到 2028 年，通过法案新措施将数据的经济价值提高至

70 到 110 亿欧元，从而使社会、公民和企业受益。

《数据治理法案》旨在促进整个欧盟内部和跨部门之间的数据共享，增强公民和公司对其数据的控制和信任，并为主要技术平台的数据处理实践提供一种新的欧洲模式，帮助释放人工智能的潜力。通过立法，欧盟将建立关于数据市场中立性的新规则，促进公共数据（例如健康、农业或环境数据）的再利用，并在战略领域创建共同的欧洲数据空间。

<https://mp.weixin.qq.com/s/DhE8ltXGgalhIqTd9KVbpA>

技术、产品与市场

1、360 核心安全大脑 3.0 正式发布，构建政企用户的“能力中枢平台”

在数字时代安全威胁不断演进的今天，对数字安全体系化、实战化提出了更高的要求。但越来越多政企用户清晰地看见——自身的网络安全建设存在着企业设备各自为战、生态产品难以联动、外部能力无法融合等多重协同壁垒。

在此背景下，360 政企安全集团正式推出 360 核心安全大脑 3.0。具体构成上，360 核心安全大脑 3.0 由一个安全大数据平台、一个云端赋能平台和多个安全分析引擎，以及内嵌 360 十七年经验所积累的实战方法论组成。其中安全大数据平台通过模型化管理的数据标准，接入各类安全数据使之集中管理，并在内部融合数据品类，协调数据流程决策与步骤，为安全业务提供从数据接入到存储、清洗到运算，最终到图表展示的全生命周期一站式服务。安全大数据平台具有“运营商”级别的数据处理能力，助力提升安全运营中的数据处理效率 5 倍以上。

云端赋能平台通过云地协同、能力下沉，为安全设备提供从漏洞到资产、从情报到知识、从线索到规则、从事件到态势等百余种基础的安全数据及分析能力，可以满足各类安

全设备的通用化威胁检测与分析需求。

此外 360 核心安全大脑 3.0 中还预置了近百类安全分析引擎，2000 多个安全策略，可以把专业相关的分析能力通过配置组合的方式赋能特定的安全产品，应对纷繁复杂的安全业务，从多个维度指导安全设备发现、防护高级别网络威胁，提升自身网络安全能力。

<https://www.anquanke.com/post/id/271594>

2、IBM 发布业界首款量子安全平台 IBM z16

近日，IBM 推出了下一代大型机系统 IBM z16，搭载人工智能处理器和量子安全系统，可为人工智能、混合云、量子计算、开源等领域提供充分支持。据 IBM 消息，IBM z16 将于今年 5 月 31 日上市。

IBM z16 集成量子安全系统，为数据安全保驾护航，除应对欺诈活动外，还可应用于诸如货币加密、贷款审核、防止盗窃等产业。IBM 以普及加密和机密计算技术为基础，采用网格密码学技术，在 IBM z16 上增加了一个保护组织免受未来技术，以破解当今加密文件威胁的量子安全系统。

<https://www.secrss.com/articles/41176>

3、《2021 年度数据泄漏态势分析报告》发布

2021 年数据泄漏事件呈现不断增长的宏观态势，尤其在 2021 年下半年，数据泄漏事件发生的频率较高，这与《数据安全法》《个人信息保护法》相继出台有一定的关系，数据安全相关法律法规将数据安全级别做出清晰划分，将前期没有意识到的情况也纳入数据泄漏范畴。

与 2020 年相比，2021 年数据泄漏所占比例进一步上升，占有所有数据安全事件类型的 80%，其中以获利为目的的数据泄漏事件占比最高，同为 80%，可见造成数据泄漏，仍然是利益驱动。

从数据的全生命周期阶段分析数据泄漏发现，2021 年数据泄漏发生在存储阶段的占比最高，接近 40%，其次是数据使用阶段，占比接近 30%，都属于数据泄漏的高风险阶段和数据安全防御的重点阶段，应给予重视。

<https://mp.weixin.qq.com/s/FD3dtOLh1hbCpe0Sui4u8Q>

4、零信任的行业应用场景分析研究

中国信通院调查分析了供应商零信任产品在各行业的应用实施情况。政府机关、信息技术服务业、金融业、制造业作为排头兵，零信任应用试点占比靠前，总占比达 53%。其原因在于，一方面，信息技术服务业是新一代信息技术发

展的最大推手，作为原生数字化企业，对零信任等新理念、技术的接受程度高；另一方面，政务、金融、制造业进入数字化转型加速阶段，云计算等新技术应用程度深，安全需求较为迫切，也积极拥抱零信任安全。

远程访问是当前企业实施零信任的主要驱动和优先选择，供应商的产品也更聚焦在该领域，远程办公、远程分支机构接入、远程运维三大场景占比居于前三，总占比达 46%。

<https://mp.weixin.qq.com/s/RgC6mhOCDQI4jBudILKdrg>

5、非可信环境下的云端数据加密与授权方案

将数据存储至云端可以有效降低用户的存储成本、提升数据共享便捷性，但在非可信环境下云端存储的数据面临诸多安全风险。虽然，数据加密能够保证数据的安全性，但却损失了数据共享的便捷性；因此，提出了一种基于格理论的属性基加密与授权方案。该方案中，数据所有者能够根据授权用户的属性设置密文策略，在数据加密的同时保证授权的灵活性。针对量子计算的发展可能带来的安全挑战，基于格构造抗量子的方案可以有效提升安全性。此外，利用区块链技术存储数据信息，以应对非可信云服务的伪造、篡改数据等行为，构建了数据完整性管理机制。

<https://mp.weixin.qq.com/s/k8vE6BFw1F2KGawIjPXq0Q>

业界观点

1、王云鹏院士：探索构建包容审慎的汽车安全监管沙盒

以 5G、大数据、云计算、人工智能等为代表的新一代信息技术与汽车产业的快速融合，由于前沿技术应用而产生的新型汽车安全问题成为社会公共安全面临的新挑战：一是汽车安全风险呈现新模式。二是汽车安全状态呈现不稳定性。三是汽车安全问题危害扩大化。

针对汽车新技术不断发展对既有安全监管体制提出的新挑战，美国、德国、韩国等发达国家开始通过建立监管沙盒，对车辆应用的前沿技术进行深度安全测试，将安全问题尽早纳入监管范围，以确保现有监管体系不会阻碍创新产品与新技术投入市场。

去年，我国国家市场监督管理总局发布《关于 2020 年全国汽车和消费品召回情况的通告》，明确“建立运行数据驱动的新能源汽车缺陷调查工作机制，推进智能汽车 OTA 大数据平台建设，探索建立智能车辆安全自我评估和事故报告制度，适时启动沙盒监管。”这是在国内汽车质量安全监管领域首次提出“沙盒监管”概念。

王云鹏表示，在汽车安全监管领域试行“沙盒监管”制度，不仅顺应了新兴产业科技发展趋势，一定程度上解决了

汽车新技术科技创新带来的监管挑战，而且能够妥善应对监管在支持创新和防控风险上的冲突，并更好地保障消费者的人身财产安全，增强消费者对产品安全的获得感，守住汽车产品安全底线。

<https://www.secrss.com/articles/41077>

2、陈兵：车企须在让渡隐私与获得便利性间找平衡点

当下，越来越多的汽车企业在后台收集并使用海量用户数据，消费者对部分汽车企业过度采集个人敏感信息的行为既担忧又无可奈何。这种“安全感”的缺失具体包括：第一，个人隐私易被监控。第二，个人财产存在风险。

陈兵认为，让渡隐私与获得便利之间的平衡点即是：“明确的个人数据信息安全保护规则”+“具体可行的产业数据安全监管与协调机制”+“合理的多元主体间利益分享机制”。他对于汽车企业该如何完善安全管理提出两个方面的建议：

一、国家层面的数据安全。汽车企业需要积极跟进国内外车联网数据安全、数据出境方面的标准、法律及监管规范的最新要求，在坚决维护国家安全和用户安全的基础上合法合规经营。

二、用户层面的数据安全与服务。汽车企业结合多种辅助数据，对用户行程轨迹、生活习惯进行“数据画像”

的行为也应有所约束。并且使用上述数据需获得用户明确授权，且原始数据信息要经过“脱敏处理”，确保不会对特定个体进行反向画像后，方能供企业分析用户需求、调整经营策略、提供增值服务，同时也要谨防头部汽车企业对车联网场景下各类智联网络数据的垄断和不正当使用。

<https://www.jwview.com/jingwei/html/04-06/476197.shtml>

3、专家解读：与时俱进 筑牢国家安全的审查防线

《网络安全法》、《数据安全法》和《个人信息保护法》三法相继生效，标志着我国的网络安全工作，从技术安全、内容安全，完成了对新维度的拓展——数据安全。

一、数据成为独立于网络的安全保护对象。随着信息技术和人类生产生活交汇融合，各类数据迅猛增长、海量聚集，对经济发展、社会治理、人民生活都产生了重大而深刻的影响。数据安全已成为事关国家安全与经济社会发展的重大问题。特别是，2018年的剑桥分析事件，震惊中外，暴露出网络和系统本身的安全，并不足以防范安全风险。

二、数据成为国际政经博弈的焦点。在《外交事务》杂志2021年发表的文章《数据即是权力》（data is power）中，两位美国作者直言：“与全球经济的其他要素相比，数据与权力更紧密地交织在一起。作为创新的一个日益必要的投入，

国际贸易的一个迅速扩大的元素，企业成功的一个重要因素，以及国家安全的一个重要层面，数据为所有拥有它的人提供了难以置信的优势。寻求反竞争优势（anticompetitive advantages）的国家和公司试图控制数据”。

三、数据成为网络安全审查的重点工作内容。新一轮数据治理中，国家不仅仅作为制度供给者，也作为独立的利益主体登场，全球数据治理立法均充分考量国家的利益诉求，各国的数据战略都服务于大数据时代的综合国力竞争，既包括维护国家安全利益的防御性诉求，也包括促进本国数字经济全球竞争，并通过规则治理抢占全球数据规则话语权。因此，从前述内外因素来看，我国《数据安全法》《个人信息保护法》，乃至新版的《网络安全审查办法》并非局限于技术安全问题，而是在更加宽泛的意义上理解数据安全，核心目的都在于保障作为基础性战略资源的数据，能够在将来被管好、用好，服务于我国的主权、安全和发展利益。

<http://news.ijntv.cn/social/2022-04-02/779124.html>

4、保护个人信息，给“算法应用”立规矩

《互联网信息服务算法推荐管理规定》（以下简称《管理规定》）近日正式施行，很多 APP 先后上线算法关闭键，允许用户在后台一键关闭“个性化推荐”。专家表示，要继

续压实平台责任，促进算法应用向上向善，让算法更好地为用户服务，推动信息服务行业长远、健康发展。

《管理规定》提出，算法推荐服务提供者向消费者销售商品或者提供服务的，应当保护消费者公平交易的权利，不得根据消费者的偏好、交易习惯等特征，利用算法在交易价格等交易条件上实施不合理的差别待遇等违法行为。

中国信息安全研究院副院长左晓栋认为，大数据“杀熟”等顽疾归根结底是滥用用户个人信息导致的。解决这类问题首先要在治理违法违规收集用户个人信息上下功夫，其次要保障用户的选择权、删除权等权益。

《管理规定》提出，算法推荐服务提供者应当定期审核、评估、验证算法机制机理、模型、数据和应用结果等，不得设置诱导用户沉迷、过度消费等违反法律法规或者违背伦理道德的算法模型。

北京大学中国社会与发展研究中心主任邱泽奇认为，在数字时代，诸多产品都是动态产品，需要根据交互数据对产品不断进行优化迭代，通过产品升级、算法升级以满足用户需求。基于人类认知偏好的复杂性，企业除了承担产品责任，还要承担起相应社会责任，把用户纳入产品的开发、生产与服务中，通过政府、企业和用户共同参与、建立相应规则，不断推动产品向善、科技向善。

《管理规定》提出“建立健全算法机制机理审核、科技伦理审查、用户注册、信息发布审核等管理制度”“提供算法推荐服务，应当遵守法律法规，尊重社会公德和伦理，遵守商业道德和职业道德”等措施。

中国社科院信息化研究中心主任姜奇平表示，从技术创新层面看，应推动算法技术回到正常轨道，比如单纯基于人们的偏好推荐阅读内容，错误之处在于对人的理解不足，把人理解成机器，没有考虑到人还具有自由意志。从价值伦理层面看，哲学上的善和伦理的本质都源于自由意志，因此应该在技术创新过程中把人之为人的的一面、人和人的关系摆进技术里考虑。

<http://tech.china.com.cn/internet/20220406/386492.shtml>

5、依法应对元宇宙发展中的风险挑战

2021年以来，围绕元宇宙的技术应用和产业投资日益成为社会关注的热点。中国社会科学院法学研究所网络与信息法研究室副主任周辉提出，需要在正确认识元宇宙发展的同时，审慎研判其带来的各类风险，提前布局治理方案。

周辉认为在元宇宙发展的过程中，如果治理措施不到位在数据安全、隐私保护方面可能出现下列风险：

一、危害网络数据安全的风险。考虑到元宇宙生产生活

场景更丰富，用户活动轨迹的全过程数字化，有关破坏性事件的突发性可能更强、波及面更广、危害性更大。元宇宙本身的跨国运营特性，也会带来频繁的用户数据出境安全问题。

二、侵害个人权益的风险。相对于既有网络平台，元宇宙生态更容易形成闭环，不同元宇宙之间互联互通的难度更大。元宇宙生态中的劳动者、消费者、经营者的权益都可能遭受侵害。

对此，周辉提出以下建议：

第一，加强依法治理、风险治理和综合治理。通过明确细化网络安全法、数据安全法、个人信息保护法等网络治理领域法律的延伸运用，为元宇宙发展划清红线、指明方向。

第二，加强统筹协调，确立牵头部门、形成跨部门协调机制，积极应对元宇宙治理跨产业、跨地域、跨国界问题，确保相关产业链供应链稳定性。

https://news.gmw.cn/2022-04/02/content_35630611.htm

数据安全事件

1、爱尔兰银行因数据泄露被罚款 463,000 欧元

2022 年 4 月 7 日，据外媒报道，爱尔兰银行因 2018 年 11 月至 2019 年 6 月期间影响客户个人信息的多项数据泄露事件被数据保护委员会 (DPC) 罚款 463,000 欧元。

该银行因违规和延迟与受影响客户沟通而被罚款。DPC 表示，报告的事件中有 19 起违反了《通用数据保护条例》(GDPR)。

https://www.infosecurity-magazine.com/news/bank-of-ireland-fined-463000-over?utm_source=twitterfeed&utm_medium=twitter

2、Lapsus\$再出手：泄露 Globant 软件公司 70GB 数据

就在英国警方逮捕了 7 名嫌疑犯之后，近期非常猖獗的黑客组织 Lapsus\$ 又有了新动作。在攻击微软、三星、NVIDIA 和 Okta 等公司之后，该组织再次宣布成功攻陷 Globant，后者是一家位于卢森堡的软件开发咨询公司。

Lapsus\$组织先在其 Telegram 频道上发布了一个 70G 的种子文件，其中包括据称从 Globant 公司窃取的数据，黑客声称其中包括其企业客户的源代码。随后 Globant 向 TechCrunch 证实，已经“检测到我们公司代码库的一个有限部分受到了未经授权的访问”，并正在进行调查。

<https://www.cnbeta.com/articles/tech/1253099.htm>

3、Conti 团伙泄露从 Parker Hannifin 窃取数 GB 文件

2022 年 4 月 5 日报道称，美国工业公司 Parker Hannifin 大量数据泄露。该公司主要为航空航天、移动和工业领域的组织提供精密工程解决方案。它在 3 月 14 日检测到系统遭到入侵，之后立刻关闭部分系统并展开调查。目前调查仍在进行中，但已确定包括员工个人信息在内的部分数据已经泄露。研究人员发现，Conti 在其数据泄露网站公开了从 Parker 窃取的超过 5GB 数据，并称这仅为被盗数据的 3%。

<https://www.securityweek.com/ransomware-gang-leaks-files-stolen-industrial-giant-parker-hannifin>

4、美国国防承包商关联公司借激励计划名头，通过 SDK 收集用户敏感数据

2022 年 4 月 8 日报道，外媒曝光了一家巴拿马公司 Measurement Systems S. de R.L，声称该公司与弗吉尼亚州的一家国防承包商 Vostrom/Packet Forensics LLC 存在关联关系，该承包商为美国国家安全机构从事网络情报、网络防御和情报截获工作。

而曝光该公司的主要原因，是由于该公司将其 SDK 代

码，通过所谓的激励计划方式，向世界各地的开发人员付费，以将其代码（软件开发工具包或 SDK）整合到他们的应用程序中，它的存在使巴拿马公司能够秘密地从数百万台 Android 设备上收集数据。

<https://www.secrss.com/articles/41130>

5、俄罗斯外卖应用的泄露数据中包含 GRU 特勤人员的用餐习惯

2022 年 4 月 4 日，据 The Verge 报道，俄罗斯外卖平台 Yandex Food 的一次大规模数据泄露暴露了属于那些与俄罗斯秘密警察有关的递送地址、电话号码、姓名和配送指示。

Yandex Food 是俄罗斯大型互联网公司 Yandex 的子公司，于 3 月 1 日首次报告了数据泄漏事件，将其归咎于其一名员工的“不诚实行为”，并指出该泄露事件不包括用户的登录信息。俄罗斯通信监管机构 Roskomnadzor 声称要对该公司的泄露行为处以最高 10 万卢布（约合人民币 7652 元）的罚款，路透社称该事件暴露了约 58000 名用户的信息。

<https://www.cnbeta.com/articles/tech/1254377.htm>

6、黑客通过虚假购物应用程序以窃取马来西亚用户的银行数据

2022 年 4 月 6 日,据外媒报道,自 2021 年 11 月以来,威胁行为者一直在以看似无害的购物应用程序为幌子分发恶意应用程序,以针对八家马来西亚银行的客户进行网络钓鱼以获取银行凭据。

这些通过 Facebook 广告分发的网站敦促访问者下载声称是 Google Play 商店上可用的 Android 应用程序,但实际上,它们将重定向到黑客控制的流氓服务器。该行为的最终目标是窃取用户输入的银行凭证并将其泄露到攻击者控制的服务器,同时显示输入的用户 ID 或密码无效的错误消息。

<https://thehackernews.com/2022/04/hackers-distributing-fake-shopping-apps.html>

7、福克斯新闻泄露 1300 万条数据,包含员工信息

2022 年 4 月 7 日,据外媒报道,配置错误暴露了数百万可追溯到福克斯新闻的内部记录,包括员工的个人身份信息。

研究人员声称,理论上任何有互联网连接的人都可以发现这个 58GB 的数据库,该数据库在没有密码保护的情况下处于暴露状态。它包含近 1300 万条内容管理数据记录,包括数量不详的员工详细信息。经过进一步研究,几乎所有记

录都包含福克斯新闻内容、存储信息、内部电子邮件、用户名、员工 ID 号、附属电台信息等。欺诈者可能利用 700 多个内部 Fox 电子邮件地址进行后续网络钓鱼攻击。

<https://www.infosecurity-magazine.com/news/employee-info-13-million-records/>

8、Cash App 数据泄露恐将影响 820 万美国用户

2022 年 4 月 7 日报道，近日，美国支付巨头 Block 披露了一项与投资应用 Cash App 有关的数据泄露事件，并将此事件告知了其 820 万美国用户。

Cash App 是一款允许用户自由转账、花钱、存钱和购买加密货币的应用程序。此次数据泄露事件中，一名 Block 的前员工被卷入其中。有证据显示，他下载了一些关于 Cash App Investing 应用程序的报告，而这其中包含了一些美国用户的信息。目前尚不清楚有多少用户受到了影响，而 Block 方面已经通知执法部门并向其大约 820 万用户告知此事。另外，公司方面宣布将继续审查和加强行政和技术保障，以保护其用户的信息。

<https://www.freebuf.com/news/327794.html>

9、得克萨斯州保险部泄露了 180 万人的数据

2022 年 4 月 6 日，据外媒报道，德克萨斯州保险部(TDI)近期披露了一起影响了大约 180 万人的数据安全事件。暴露的信息包括姓名、地址、电话号码、出生日期、部分或全部社会安全号码，以及有关工伤和工人赔偿要求的信息。

“我们发现该安全事件是由于编程代码允许互联网访问 Web 应用程序的受保护区域。”该组织表示。目前尚不清楚这些数据暴露了多长时间，但 TDI 声称没有目前发现任何数据滥用的证据。

https://www.securityweek.com/texas-department-insurance-exposed-data-18-million-people?&web_view=true

10、西班牙 Iberdrola 遭到攻击泄露 130 万客户的数据

2022 年 4 月 4 日消息，西班牙能源公司 Iberdrola 泄露了 130 万客户的个人信息。该公司已证实，他们在 3 月 15 日遭到网络攻击，黑客非法访问了客户的身份证号码、地址、电话号码和邮件地址等信息。Iberdrola 表示，该问题已在当天被修复，其成功阻止了进一步的攻击，但还是提醒客户注意利用这些信息的钓鱼活动。

<https://www.infosecurity-magazine.com/news/scottish-power-parent-data->

[breach?utm_source=twitterfeed&utm_medium=twitter](#)